Inventors: Sherry L. Krell and Sergey V. Gerasimov
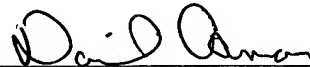
A METHOD AND APPARATUS FOR
SEEDING A RANDOM NUMBER GENERATOR

1   A METHOD AND APPARATUS FOR
2   SEEDING A RANDOM NUMBER GENERATOR

3   SUMMARY OF THE INVENTION

4   The present invention relates generally to the operation of computer

5   systems and more specifically to the generation of random or pseudo-random

6   numbers in computer systems.

7   In the operation of computer systems, it is often desirable to generate

8   random numbers for use in certain applications such as simulations, games, and

9   secure communications. A random number is a sequence of numbers in which

10   no number is more likely to occur at a given place in the sequence than any

11   other number. Generation of a truly random number is generally considered to

12   be impossible, but computer processes may generate numbers called "pseudo-

13   random numbers" that are sufficiently unpredictable to serve an intended

14   purpose.   These pseudo-random numbers are hereinafter called "random

15   numbers," and their generation "random number generation," in conformance

16   with common usage.

17   One prior method of generating random numbers in a computer system

18   relies on the collection of random data over time from the computer system

19   itself for use as a seed, i.e., a starting value used in generating random

20   numbers, for a random number generator. Another prior method relies directly

1   or indirectly on user interaction via, e.g., a keyboard or mouse, for random data

2   to use as a random number generator seed.

3   In some circumstances, however, user input is not available, for

4   example, for embedded devices requiring no user interaction and having no

5   user interfaces. Further, if one or more random numbers are required in a short

6   time, for example, almost immediately after startup, there may not be enough

7   time for the collection of random data for a seed. In addition, where the

8   resources from which random data may be gathered are limited, for example in

9   the limited memory of an embedded device, the data available may be

10   insufficient to provide enough random data for a random number generator

11   seed.

12   BRIEF DESCRIPTION OF THE DRAWINGS

13   FIGURE 1 is a flowchart showing an embodiment of the invention;

14   FIG. 2 is a flowchart showing another embodiment of the invention; and

15   FIG. 3 is a block diagram of an embodiment of the invention.

16   DETAILED DESCRIPTION

17   Broadly stated, the present invention is directed to apparatus and

18   methods for seeding a random number generator in a computer system without

19   user interaction, network connection, or an elapsed period of time to collect

1   data to form a seed, allowing a requirement for a random number to be fulfilled

2   by a random number generator in a relatively short time, e.g., immediately after

3   power-up of a computer device.

4   Turning now to FIG. 1, showing a flowchart for an embodiment of the

5   invention, a first data block is retrieved from memory (10). The first retrieved

6   data block may include but is not limited to previously stored data or a unique

7   identifier for a device or component such as a media access control ("MAC")

8   address. A random number generator is initially seeded with the retrieved first

9   data block (12). The random number generator generates a number and that

10   number is retrieved (14). The generated number is mapped to a memory

11   address using a mathematical function (16). A successive memory block is

12   retrieved starting at the memory address to which the generated number was

13   mapped (18).

14   The successive data block retrieved by step 18 is tested for satisfaction

15   of at least one criterion for the suitability of the seed (20), and if the at least one

16   criterion is not satisfied, steps 14, 16, 18, and 20 are repeated until the at least

17   one criterion is satisfied. In embodiments of the invention in which step 20

18   tests for satisfaction of more than one criterion, the testing may be satisfied if

19   one, some, or all of the criteria are satisfied, depending on the application in

20   which the embodiments are being used. Use of the phrase "at least one

21   criterion" is not intended to limit embodiments of the invention to satisfaction

1   of only one of a plurality of criteria when a plurality of criteria are employed.

2   When the at least one criterion is satisfied, the successive memory block

3   and the seed are combined, and the combination becomes the resulting seed of

4   the random number generator (22). The combination of the successive memory

5   block and the seed may be accomplished by hashing the successive memory

6   block and the seed but is not limited to that method.

7   In an embodiment of the invention, the mathematical function of step 16

8   is:

9         $f(x) = x \pmod{m} + b$ for $x < b$;

10        $f(x) = x$ for $b \leq x \leq b + m$; and

11        $f(x) = x \pmod{m} + b$ for $x > b + m$;

12   where x = retrieved number generated by random number generator; b = base

13   memory address; and m = memory size. The base memory address is the

14   address at which the memory available to this embodiment of the invention

15   begins, and the memory size is the size of that available memory.

16   In an embodiment of the invention, the at least one criterion of step 20

17   includes an absence of a string of identical bits in said successive data block

18   longer than a specified number of bits. In an embodiment of the invention, that

19   number may the equal to the number of bits in the successive data block.

20   Turning now to FIG. 2, showing another embodiment of the invention,

21   steps 10, 12, 14, 16, 18, 20, and 22 are as described in connection with FIG. 1.

1   The successive data block retrieved from memory in step 18 is tested for

2   satisfaction of one or more second criteria (20). If the at least one criterion is

3   not satisfied, a determination is made of the number of times steps 14, 16, 18,

4   and 20 have been repeated due to failure to satisfy the at least one criterion

5   (24). If the number of repetitions of steps 14, 16, 18, and 20 is less than a

6   specified number (e.g., two), steps 14, 16, 18, and 20 are repeated. If step 20

7   determines that the at least one criterion has been satisfied before step 24

8   determines that the specified number of repetitions has been accomplished, the

9   next step after step 20 is step 22. If step 24 determines that the specified

10 number of repetitions has been accomplished before step 20 determines that the

11 at least one criterion has been satisfied, the next step after step 24 is step 22.

12   Turning now to FIG. 3, showing an embodiment of the invention, an

13 apparatus includes a memory 26 and a processor 28. The processor 28 is

14 programmed to (a) retrieve a first data block from a memory; (b) initially seed

15 the random number generator using the first data block as a seed; (c) retrieve a

16 number generated by the random number generator; (d) map the number to a

17 memory address in the memory using a mathematical function; (e) retrieve a

18 successive data block from the memory address; and (f) successively seed the

19 random number generator with a combination of the seed and the successive

20 data block such that the combination of the seed and the successive data block

21 becomes the resulting seed.

1   In an embodiment of the invention, the processor 28 is further

2   programmed to perform the further step, defined as (e'), which is to test, after

3   each performance of (e), for satisfaction of at least one criterion and if the at

4   least one criterion is not satisfied, repeat steps (c), (d), (e), and (e').

5   In an embodiment of the invention in which the processor 28 is

6   programmed to perform step (e') as described above, the processor 28 is further

7   programmed to perform the further step, defined as (e"), which is to check,

8   after each performance of (e'), the number of repetitions of steps (c), (d), (e),

9   and (e') due to failure to satisfy the at least one criterion and stop the

10   repetitions when a specified number of the repetitions have been performed.

11   While various embodiments of the present invention have been shown

12   and described, it should be understood that other modifications, substitutions,

13   and alternatives are apparent to one of ordinary skill in the art. Such

14   modifications, substitutions, and alternatives can be made without departing

15   from the spirit and scope of the invention, which should be determined from

16   the appended claims.

17   Various features of the present invention are set forth in the appended

18   claims.